PHILLIP A. TALBERT
Acting United States Attorney
KEVIN C. KHASIGIAN
Assistant U. S. Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700

Attorneys for the United States

IN THE UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 10.19321397 BITCOIN, Defendant.	VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America, by and through its undersigned attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions:

NATURE OF ACTION

1. This is a civil action *in rem* to forfeit to the United States Approximately 10.19321397 Bitcoin (hereafter "defendant cryptocurrency") involved in violations of wire fraud.

2. The defendant cryptocurrency was seized by the U.S. Secret Service ("USSS") on or about September 21, 2021, pursuant to a Federal seizure warrant. The defendant cryptocurrency is currently in the custody of the USSS in Washington D.C.

JURISDICTION AND VENUE

3. This Court has jurisdiction over an action commenced by the United States under

28 U.S.C. § 1345, over an action for forfeiture under 28 U.S.C. § 1355(a).

4. This district is a proper venue pursuant to 28 U.S.C. § 1355 and 28 U.S.C. § 1395 because the acts or omissions giving rise to the forfeiture occurred in this district.

FACTUAL ALLEGATIONS

5. The USSS began an investigation into a fraud scheme that took place on or around February 7, 2021, targeting a single known victim who resides in Oroville, California (hereinafter "Victim 1"). As a result of the scheme, this individual was defrauded out of approximately 12.51 Bitcoin ("BTC").

6. The USSS was notified of a potential fraud on April 6, 2021. The USSS agent believes an individual attempted to defraud others via a fake cryptocurrency wallet site that mirrored the legitimate one (https://trezor[.]io) in order to defraud unassuming individuals.[1] The fake Trezor site could be found by searching for "trezor.io wallet" on the Bing search engine. Victim 1 accessed the fake site and provided the likely fraudster with their "mnemonic key.[2]" These words, when listed in the correct order on the legitimate Trezor, allowed the likely fraudster who created the fake website to re-create the victim wallet and drain approximately 12.51 BTC from it.

7. An examination of Victim 1's browser history on February 7, 2021 shows that Victim 1 conducted a Bing search and then accessed a site titled "Trezor Hardware Wallet (official) | The original and most secure hardware wallet." After accessing it, Victim 1's browser history indicates that they were re-directed to another site (https://trrezorr[.]io/start). Once on the fake Trezor site, Victim 1 was asked to type in their "mnemonic key." Doing so gave the fraudster access to all cryptocurrency in Victim 1's wallet.

8. Analysis of victim 1's Trezor wallet shows that there were multiple deposits made into the wallet. The initial deposit was on December 17, 2017 and the final one was on August 12, 2019. On August 12, 2019, the balance in the victim's wallet was approximately 12.51 BTC. Blockchain analysis and Victim 1's Trezor transaction history shows that shortly after they accessed the fake Trezor site, approximately 12.51 BTC was removed from the victim's Trezor wallet. Victim 1 stated that they did

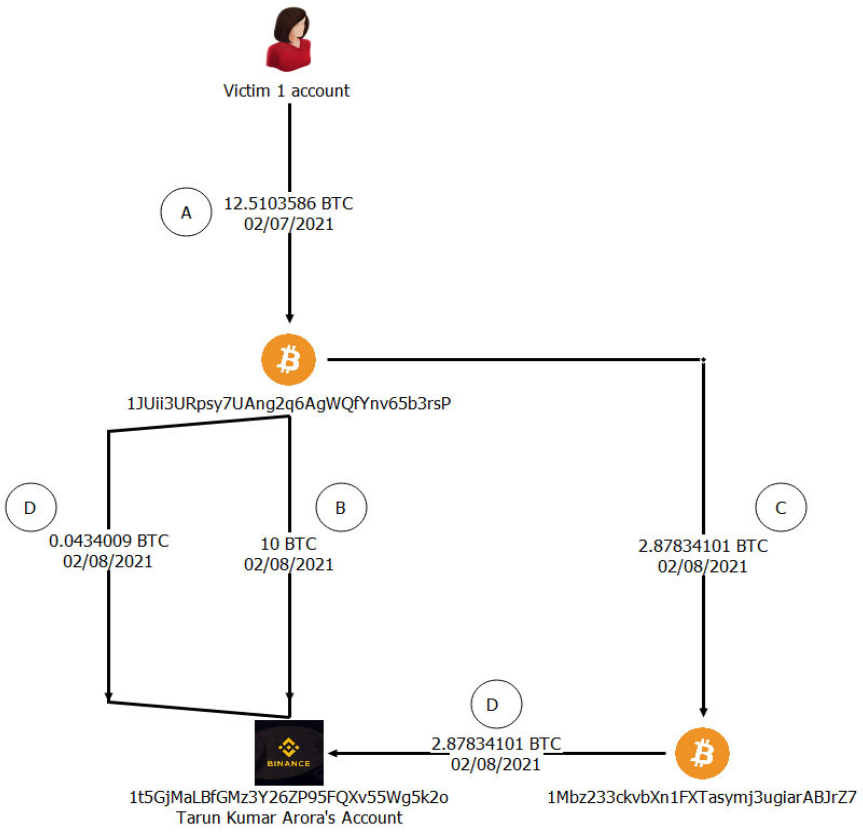
[1] Trezor is a company that makes "wallets" used to store cryptocurrency.

[2] This mnemonic key contains all of the information required to regenerate a Trezor Wallet. As a result, gaining access to a device's mnemonic key is similar to having its password.

not initiate this transaction. The approximately 12.51 BTC was sent to a wallet known as 1JUii3URpsy7UAng2q6AgWQfYnv65b3rsP (herein, "1JUii"). The approximately 12.51 BTC was then co-mingled with other funds of unknown origin and ultimately deposited into the account of Tarun Kumar Arora at Binance cryptocurrency exchange.

9. The USSS agent believes the fraudster sent Victim 1's BTC to Binance. Through blockchain tracing analysis, the agent has determined that Victim 1's BTC was sent to Tarun Kumar Arora at Binance Cryptocurrency exchange ("the Arora Binance Account"). Specifically, on February 7, 2021, the approximately 12.51 in stolen BTC was transferred out of Victim 1's Trezor wallet and to at least one intermediary address (described in detail below). It was then transferred almost entirely to Arora at Binance.

10. The below illustration shows the movement of BTC from Victim 1's wallet to Arora's Binance account.



a. On February 7, 2021, Victim 1's Trezor wallet sent BTC to address[3] 1JUii (totaling approximately 12.51 BTC). This 12.51 BTC was then co-mingled with approximately .043 BTC from another address. The source of the .043 BTC is unknown and not derived from the victim account.

b. On February 8, 2021, address 1JUii transferred approximately 10 BTC from Victim 1 to 1t5GjMaLBfGMz3Y26ZP95FQXv55Wg5k2o (herein, 1t5Gj).

c. Then, approximately 2.51 BTC from 1JUii along with an additional approximately .36 BTC from other addresses (totaling approximately 2.87 BTC was sent to 1Mbz233ckvbXn1FXTasymj3ugiarABJrZ7 (herein, 1Mbz2). Analysis has shown that the same likely fraudster controls both 1JUii and 1Mbz2.

d. On the same day (February 8, 2021), virtually all of the remaining approximately .043 BTC left in 1JUii along with the approximately 2.87 BTC from 1Mbz2 (totaling approximately 2.92 BTC) was sent to address 1t5Gj.[4]

11. The USSS agent confirmed that the account containing the stolen BTC is Arora's based upon information provided by Binance. They have confirmed that 1t5Gj is associated to Tarun Kumar Arora at their exchange because Arora has provided Binance with "Know Your Customer (KYC)" information. This KYC information included a "selfie" and Indian passport with matching photo. Arora provided Binance an email address (xxxxx_0085@rediffmail.com) from which customer service requests have been placed. An individual who identified himself as Arora also emailed the USSS agent from email address xxxxxx3335@gmail.com, requesting that his Binance account be unlocked and that he was willing to speak with law enforcement about the matter. The USSS agent emailed Arora on September 8, 2021 but did not get a response from him until October 15, 2021.

12. As noted above, the stolen BTC was held in an account at Binance. Binance is headquartered at Level 3, Melita Court, Triq Giuseppe Cali, Ta'Xbiex XBX 1420, Malta. The USSS agent identified that users who hold accounts on the Binance platform login to it through the main

[3] An address is somewhat analogous to a bank account number and is comprised of a case-sensitive string of letters and numbers amounting to a total of 26-35 characters.

[4] Mixing and co-mingling of BTC is commonly used by fraudsters to intentionally obscure the movement of stolen cryptocurrency.

website https://www.binance[.]com or via web-based application. Account User ID/User ID# 25002089/ R8750839, held in the name of Tarun Kumar Arora, was first frozen by Binance at the request of the USSS. On September 21, 2021, a Federal seizure warrant was executed on Binance for the virtual currencies currently held in User ID 25002089/User ID Number R8750839, controlled by and in the name of Tarun Kumar Arora, at the virtual currency exchange Binance. Approximately 10.19321397 Bitcoin (the defendant cryptocurrency) was seized from Binance pursuant to the Federal seizure warrant.

FIRST CLAIM FOR RELIEF
18 U.S.C. § 981(a)(1)(C)

13. The above paragraphs are incorporated by reference as though fully set forth herein.

14. The United States alleges that the defendant cryptocurrency was derived from proceeds traceable to an offense constituting a "specified unlawful activity" as defined in 18 U.S.C. § 1956(c)(7), which incorporates the definition of "specified unlawful activity" found in 18 U.S.C. § 1961(1) and is therefore subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C). Wire Fraud in violation of 18 U.S.C. § 1343, constitutes "specified unlawful activity" as defined in § 1961(1).

PRAYER FOR RELIEF

WHEREFORE, the United States prays that:

1. Process issue according to the procedures of this Court in cases of actions *in rem;*

2. Any person having an interest in said defendant cryptocurrency be given notice to file a claim and to answer the complaint;

3. The Court enter a judgment of forfeiture of the defendant cryptocurrency to the United States; and

4. The Court grant such other relief as may be proper.

DATED: 12/17/2021

PHILLIP A. TALBERT
Acting United States Attorney

By: /s/ Kevin C. Khasigian
KEVIN C. KHASIGIAN
Assistant U.S. Attorney

VERIFICATION

I, Andrew Foss, hereby verify and declare under penalty of perjury that I am a Special Agent with the U.S. Department of Homeland Security, United States Secret Service, that I have read the foregoing Verified Complaint for Forfeiture *In Rem* and know the contents thereof, and that the matters contained in the Verified Complaint are true to the best of my knowledge and belief.

The sources of my knowledge and information and the grounds of my belief are official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent with the United States Secret Service.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated: 12/17/21

ANDREW FOSS
Special Agent
U.S. Department of Homeland Security
United States Secret Service